STATE OF SOUTH DAKOTA
OFFICE OF PROCUREMENT MANAGEMENT
523 EAST CAPITOL AVENUE
PIERRE, SOUTH DAKOTA 57501-3182

Department of Social Services Time Study Sampling System

Proposals are due no later than March 13, 2015 5:00 pm CDT

RFP #20

BUYER: Division of Finance
& Management

POC: Mark Close
mark.close@state.sd.us

READ CAREFULLY

FIRM NAME: ____________________ AUTHORIZED SIGNATURE: ____________________

ADDRESS: ____________________ TYPE OR PRINT NAME: ____________________

CITY/STATE: ____________________ TELEPHONE NO: ____________________

ZIP (9 DIGIT): ____________________ FAX NO: ____________________

FEDERAL TAX ID#: ____________________ E-MAIL: ____________________

PRIMARY OFFEROR CONTACT INFORMATION

CONTACT NAME: ____________________ TELEPHONE NO: ____________________

FAX NO: ____________________ E-MAIL: ____________________

1.0 GENERAL INFORMATION

1.1 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

The purpose of this RFP is to procure a hosted timekeeping sampling system. The system must be capable of two types of timekeeping sampling: random moment, and 17 random day. The system must produce appropriate reports sufficient for the Department to make proper allocations.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Division of Finance & Management is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Social Services. The reference number for the transaction is RFP #20. Refer to this number on all proposals, correspondence, and documentation relating to the RFP.

Please refer to the Department of Social Services website link http://dss.sd.gov/rfp/index.asp for the RFP, any related questions/answers, changes to schedule of activities, amendments, etc.

1.3 LETTER OF INTENT

All interested offerors are requested to submit a non-binding **Letter of Intent** to respond to this RFP. While preferred, a Letter of Intent is not mandatory to submit a proposal.

The letter of intent must be received by email in the Department of Social Services by no later than February 6, 2015 and must be addressed to Mark Close at mark.close@state.sd.us. Place the following in the subject line of your email: **Letter of Intent for RFP #20.** Be sure to reference the RFP number in any attached letter or document.

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	01/26/2015
Letter of Intent to Respond Due	02/06/2015
Deadline for Submission of Written Inquiries	02/18/2015
Responses to Offeror Questions	03/03/2015
Proposal Submission	**03/13/2015 by 5:00 pm CDT**
Oral Presentations/discussions (if required)	To be announced, if needed
Deadline for Completion of Site Visits (if required)	To be announced, if needed
Proposal Revisions (if required)	To be announced, if needed
Anticipated Award Decision/Contract Negotiation	04/07/2015

1.5 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received in the Department of Social Services by the date and time indicated in the Schedule of Activities.

Proposals received after the deadline will be late and ineligible for consideration.

An original, 5 identical copies, and 1 digital copy of the proposal including all attachments must be submitted in accordance with Section 5.1.

All proposals must be signed in ink by an officer of the responder legally authorized to bind the responder to the proposal, and sealed in the form intended by the respondent. Proposals that are not properly signed may be rejected. The sealed envelope must be marked with the appropriate RFP

Number and Title. The words “Sealed Proposal Enclosed” must be prominently denoted on the outside of the shipping container. **Proposals must be addressed and labeled as follows:**

Request For Proposal #20 Proposal Due March 13, 2015
South Dakota Department of Social Services
Attention: Mark Close
700 Governors Drive
Pierre SD 57501-2291

No punctuation is used in the address. The above address as displayed should be the only information in the address field.

No proposal may be accepted from, or any contract or purchase order awarded to any person, firm or corporation that is in arrears upon any obligations to the State of South Dakota, or that otherwise may be deemed irresponsible or unreliable by the State of South Dakota.

1.6 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION – LOWER TIER COVERED TRANSACTIONS

By signing and submitting this proposal, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds. Where the offeror is unable to certify to any of the statements in this certification, the bidder shall attach an explanation to their offer.

1.7 NON-DISCRIMINATION STATEMENT

The State of South Dakota requires that all contractors, vendors, and suppliers doing business with any State agency, department, or institution, provide a statement of non-discrimination. By signing and submitting their proposal, the offeror certifies they do not discriminate in their employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.8 MODIFICATION OR WITHDRAWAL OF PROPOSALS

Proposals may be modified or withdrawn by the offeror prior to the established due date and time.

No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered.

1.9 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after the date and time indicated in the Schedule of Activities. Email inquiries must be sent to Mark Close at mark.close@state.sd.us with the subject line “RFP #20.

The Department of Social Services will respond to offeror’s inquiries by posting all offeror aggregated questions and Department of Social Services’ responses on the DSS website at http://dss.sd.gov/rfp/index.asp no later than March 3, 2015. Offerors may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.10 PROPRIETARY INFORMATION

The proposal of the successful offeror(s) becomes public information. Proprietary information can be protected under limited circumstances such as client lists and non-public financial statements.

Pricing and service elements are not considered proprietary. An entire proposal may not be marked as proprietary. Offerors must clearly identify in the Executive Summary and mark in the body of the proposal any specific proprietary information they are requesting to be protected. The Executive Summary must contain specific justification explaining why the information is to be protected. Proposals may be reviewed and evaluated by any person at the discretion of the State. All materials submitted become the property of the State of South Dakota and may be returned only at the State's option.

1.11 LENGTH OF CONTRACT

The contract will run from the award date to the end of the state fiscal year. Annual renewal will be an option at the beginning of the following fiscal year.

1.12 GOVERNING LAW

Venue for any and all legal action regarding or arising out of the transaction covered herein shall be solely in the State of South Dakota. The laws of South Dakota shall govern this transaction.

1.13 DISCUSSIONS WITH OFFERORS (ORAL PRESENTATION/NEGOTIATIONS)

An oral presentation by an offeror to clarify a proposal may be required at the sole discretion of the State. However, the State may award a contract based on the initial proposals received without discussion with the offeror. If oral presentations are required, they will be scheduled after the submission of proposals. Oral presentations will be made at the offeror's expense.

This process is a Request for Proposal/Competitive Negotiation process. Each Proposal shall be evaluated, and each respondent shall be available for negotiation meetings at the State's request. The State reserves the right to negotiate on any and/or all components of every proposal submitted. From the time the proposals are submitted until the formal award of a contract, each proposal is considered a working document and as such, will be kept confidential. The negotiation discussions will also be held as confidential until such time as the award is completed.

2.0 STANDARD AGREEMENT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State's standard terms and conditions as seen in Attachment A: Depending on the selected solution, certain provisions in the contract my no be applicable and terms of the contract will be negotiated.

3.0 SCOPE OF WORK

3.1 Background

3.1.1 Within the Department of Social Services various time study systems have been established to determine the accurate amount of costs to allocate to each cost center. The following methodologies of time study are used in the department:

- Cost Allocation Time Study (CATS)
- Time Keeping System Time Study (TKS)
- Random Moment Sample Time Study (RMS)

3.1.2 The units that complete the CATS time study system for cost allocation purposes are: Recoveries & Investigations, Child Protection Services Administration, Provider Reimbursement and Auditing, Administrative Hearings, Auxiliary Placement Support Staff, Quality Control, Economic Assistance Administration, Electronic Benefits Transfer, Adult Services and Aging Administration, Victims Services Administration, and Tribal Social Workers under contract for Child Protection Services. All units completing the CATS time study complete a time study for one month out of a quarter. For these staff to complete times studies that are statistically valid would impose an undue reporting burden on them. As an alternative, The Division of Cost Allocation (HHS) proposed that these units will complete time study forms for an entire month out of each quarter. The second month out of each quarter is designated as the time study month for all units participating in the time study. The CATS timekeeping system sampling observations is based on minutes worked during one selected month of each quarter for 68 employees. The Department would like to change these units to 17 random days.

3.1.3 DSS requires administrative staff employees for the Division of Community Behavioral Health Services to complete time studies for 17 randomly selected days each quarter. Each employee is required to keep track of their time and enter the appropriate hours/minutes into the Bureau of Human Resources TKS Timeform / Timestudy system. The TKS timekeeping system samples minutes worked during 17 random days each quarter for 20 employees.

3.1.4 Random Moment Sampling (RMS) is a statistical method for determining the percentage of time which workers expend on specific programs and activities in which they are engaged. It is a valid and cost effective alternative to other methods of measuring the application of time applied to specific activities, such as time sheets or activity logs. The employees included in this data base are all positions performing directly related program functions benefiting one or more program or service area including Economic Assistance field offices, Adult Services and Aging field offices, and Child Protection Services field offices with the exception of positions performing clerical support functions and direct services. Each sample period this data base is updated so that the sample accurately reflects the activity of all employees in these programs. SAMPLE SIZE The sample size for RMS the entire State is 4,600 observations (2 distinct 2,300 samples) per quarter for group from services workers sample population EA 217 employees, ASA 69 employees and CPS 209 employees.

3.1.5 This project involves obtaining a Random Moment Timestudy system that will replace the existing Random Moment Timestudy system for the Department of Social Services.

3.1.6 This project involves obtaining a hosted 17 Random Day Timestudy system that will replace multiple existing systems for the Department of Social Services.

3.2 Describe your proposed timestudy system and how it would meet our agencies needs.

3.3 Describe the role of the participants in the system and how they would access the system.

3.4 Describe the role of the Department of Social Service’s staff in charge of systems. Identify how they would add additional areas to tracking within each grant, notification to non-responding participants, access the system reports and other required responsibilities. Describe your user administration hierarchy, rights, and permissions for Department of Social Services management staff.

3.5 The system must meet the following regulation and standards. Describe how your system complies with the following requirements:

(a) Conforms to two Code of Federal Regulations: Part 225 and 45 CFR Part 95.
(b) Software must be capable of designing sample selections to permit a precision level of +/- 2% with a 95% confidence level for activities with expected rates of occurrence of at least 5%. For expected rates of occurrence less than 5%, precision is reduced to +/- 5%. However, the confidence level will remain at 95% regardless of the expected rate of occurrence.
(c) System must be able to quantify sample results at the end of each quarter sufficient for DSS staff to use in allocating costs to over 60 state and federal programs.
(d) Describe your service level agreement and operation up time %.

3.6 The system sought should include the following capabilities. Describe how your system compares:

(a) Describe your data backup process and recovery ability, and expected recovery times.
(b) Must easily be able to retrieve and print reports within the system.
(c) Provide an electronic form designer that is flexible and can easily create, modify, and maintain forms by the user.
(d) Ability to create, export, and print forms electronically in Excel and/or PDF formats, at a minimum, including timestudy data.
(e) Provide the ability to load and update staff pools and participant rosters in the RMTS system.
(f) Send copies of "Response Needed" lists regarding study participants that have not responded within 48 hours after the original sample date/time on a daily basis with all non-respondents identified and provided on time to the State.

3.7 How does your system meet the Sample requirements

3.7.1 Timestudy Sample Reporting Quarter - the timestudies are to be completed on a quarterly basis as follows:

a. First Calendar Quarter = January, February, March
b. Second Calendar Quarter = April, May, June
c. Third Calendar Quarter = July, August, September
d. Fourth Calendar Quarter = October, November, December

3.7.2 Core Work Hours

The sample must be selected during the agency core work hours of 8:00 am to 5:00 pm Central time and Mountain Time. The actual agency hours are used regardless of the agency's flexible work hours. For offices using flex time, the core work hours in which the majority of staff is scheduled to work are used. The timestudy will need to account for multiple time zones.

3.7.3 Sample Selection: The quarterly sample must be random and cannot be changed until the next sample is selected.

3.8 Training Requirements – describe what your company offers

3.8.1 The offeror must provide initial system training to approximately (3) department administrators. Training must be completed four (4) weeks prior to the first sample quarter.

3.8.2 The offeror must provide initial web-based, on-demand training to approximately 600 DSS staff and management. Training must be made available three (3) weeks prior to the first sample quarter. The offeror must ensure that the system does not accept responses from participants who have not completed this training.

3.8.3 During the term of the contract, the offeror must provide annual, on-demand, web-based training to all timestudy participants, plus online training for all new workers added to the quarterly rosters. The objective of this training is to ensure timestudy participants understand the RMTS process, the role it plays in the Department of Social Services, and its applicability to their daily tasks.

3.9 Auditing – How does your company meet system auditing requirements

.

3.9.1 Describe the approach to validate statistical accuracy and precision

3.9.2 The current timekeeping systems are used to document the activities by staff performing directly related program functions benefitting one or more Federal and/or State funded programs. The information collected will be used for distributing the cost of administrative activities among various programs and services. Program funding for each quarter will be based upon the data processed from the Timestudy results.

3.9.3 (a) Retention of audit documentation. Audit documentation and reports must be retrievable for a minimum of three years after the date of issuance of the auditor's report(s). (5 years)

3.9.4 (b) Access to audit documentation. Audit documentation must be made available upon request. Access to audit documentation includes the right of Federal agencies to obtain copies of audit documentation, as is reasonable and necessary. (Code of Federal Regulations / Title 2 - Grants and Agreements / Vol. 1 / 2014-01-01186)

3.9.5 The system must require that all changes to information resources are documented and stored on a secure server. All users must be uniquely identified. Group or shared IDs are prohibited. The following minimum set of events/actions must be logged and kept as required by state and federal laws/regulations:

1. Additions, changes or deletions to data produced by IT systems;
2. Identification and authentication processes;
3. Actions performed by system operators, system managers, system engineers, technical support, data security officers, and system administrators and system end users; and
4. Emergency actions performed by support personnel and highly privileged system and security resources.

3.9.6 Audit trails must include at least the following information:

1. Date and time of event.
2. User ID of person performing the action.
3. Type of event.
4. Asset or resource name and type of access.
5. Success or failure of event.
6. Source (terminal, port, location, IP address) where technically feasible.
7. Identification and authentication processes.
8. The system must follow minimum auditing requirements to be in compliance with federal requirements as defined by the United States Department of Health and Human Services.

4.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

4.1 The offeror is cautioned that it is the offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal.

4.2 **Offeror's Contacts**: Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all of their questions or comments regarding the RFP, the evaluation, etc. to the buyer of record indicated on the first page of this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the buyer of record.

4.3 Please describe the resources available to help set up the initial system and the ongoing staff available for any system questions that may arise. Provide a copy of your organizational structure.

4.4 What does past your past history show on how long it takes to transition to a new system?

4.5 Provide a list of potential problems/risks that organization have encountered during similar projects. Provide how such problems/risks solved by your company.

4.6 The offeror **MUST** submit a copy of their most recent independently audited financial statements.

4.7 The offeror must submit screen shot and/or test environment of timestudy system entry and reports.

4.8 Provide the following information related to at least three previous and current service/contracts performed by the offeror's organization which are similar to the requirements of this RFP. Provide this information for any service/contract that has been terminated, expired or not renewed in the past three years:

a. Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted;
b. Dates of the service/contract; and
c. A brief, written description of the specific prior services performed and requirements thereof.

4.9 Provide a record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;

4.10 The offeror must submit information that demonstrates their availability and familiarity with the project locale.

4.11 The offeror must detail examples that document their ability and proven history in handling special project constraints.

4.12 Offeror must detail their proposed project management techniques for implementing this project.

4.13 If an offeror's proposal is not accepted by the State, the proposal will not be reviewed/evaluated.

5.0 PROPOSAL RESPONSE FORMAT

5.1 An original and 5 copies shall be submitted.

5.1.1 In addition, the offeror must provide one (1) copy of their entire proposal, including all attachments, in PDF electronic format. Offerors may not send the electronically formatted copy of their proposal via email.

5.1.2 The proposal should be page numbered and should have an index and/or a table of contents referencing the appropriate page number.

5.2 All proposals must be organized and tabbed with labels for the following headings:

5.2.1 **RFP Form**. The State's Request for Proposal form completed and signed.

5.2.2 **Executive Summary.** The one or two page executive summary is to briefly describe the offeror's proposal. This summary should highlight the major features of the proposal. It must indicate any requirements that cannot be met by the offeror. The reader should be able to determine the essence of the proposal by reading the executive summary. Proprietary information requests should be identified in this section.

5.2.3 **Detailed Response.** This section should constitute the major portion of the proposal and must contain at least the following information:

5.2.3.1 A complete narrative of the offeror's assessment of the work to be performed, the offeror's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the offeror's understanding of the desired overall performance expectations.

5.2.3.2 A specific point-by-point response, in the order listed, to each requirement detailed in sections 3 and 4 in the RFP. The response should identify each requirement being addressed as enumerated in the RFP.

5.2.3.3 A clear description of any options or alternatives proposed.

5.2.4 **Cost Proposal.** Cost will be evaluated independently from the technical proposal. Offerors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.

See section 7.0 for more information related to the cost proposal.

6.0 PROPOSAL EVALUATION AND AWARD PROCESS

6.1 After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria as listed in relative ranking of importance:

6.1.1 Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;

6.1.2 Resources available to perform the work, including any specialized services, within the specified time limits for the project;

6.1.3 Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;

6.1.4 Cost proposal.
6.1.5 Proposed project management techniques;

6.1.6 Ability and proven history in handling special project constraints, and

6.1.7 Availability to the project locale;

6.1.8 Familiarity with the project locale;

6.2 Experience and reliability of the offeror's organization are considered subjectively in the evaluation process. Therefore, the offeror is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.

6.3 The qualifications of the personnel proposed by the offeror to perform the requirements of this RFP, whether from the offeror's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

6.4 The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota.

6.5 **Award:** The requesting agency and the highest ranked offeror shall mutually discuss and refine the scope of services for the project and shall negotiate terms, including compensation and performance schedule.

6.5.1 If the agency and the highest ranked offeror are unable for any reason to negotiate a contract at a compensation level that is reasonable and fair to the agency, the agency shall, either orally or in writing, terminate negotiations with the contractor. The agency may then negotiate with the next highest ranked contractor.

6.5.2 The negotiation process may continue through successive offerors, according to agency ranking, until an agreement is reached or the agency terminates the contracting process.

7.0 COST PROPOSAL

Startup cost (1st year)	
Ongoing Yearly Support and Maintenance Fee	
Fixed hourly development rate for any future development	
Contract terms and conditions	
Warranty of service	

Attachment A

STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
DIVISION OF FINANCE AND MANAGEMENT

Consultant Contract
For Consultant Services
Between

State of South Dakota
Department of Social Services
Division of Finance and Management
700 Governors Drive
Pierre, SD 57501-2291

______________________________	______________________________
Referred to as Consultant	Referred to as State

<u>The State hereby enters into a contract for consultant services with the Consultant. While performing services hereunder, Consultant is an independent contractor and not an officer, agent, or employee of the State of South Dakota.</u>

1. **CONSULTANT'S South Dakota Vendor Number is __________________________ .**

2. PERIOD OF PERFORMANCE:
   A. This Agreement shall be effective as of ________and shall end on _______, unless sooner terminated pursuant to the terms hereof.

   B. Agreement is the result of request for proposal process, RFP #20.

3. PROVISIONS:
   A. <u>The Purpose of this Consultant contract:</u>
      1.

   B. <u>The Consultant agrees to perform the following services (add an attachment if needed.):</u>
      1.

   C. <u>The State agrees to:</u>
      1.

      2. Make payment for services upon satisfactory completion of services and receipt of bill. Payment will be in accordance with SDCL 5-26.

      3. Will the State pay Consultant expenses as a separate item?
         NO

   D. The TOTAL CONTRACT AMOUNT will not exceed **$_______________.**

4. BILLING:
Consultant agrees to submit a bill for services within (30) days following the month in which services were provided. Consultant will prepare and submit a monthly bill for services. Consultant agrees to submit a final bill within 45 days of the contract end date to receive payment for completed services. If a final bill cannot be submitted in 45 days, then a written request for extension of time and explanation must be provided to the State.

5. TECHNICAL ASSISTANCE:
The State agrees to provide technical assistance regarding Department of Social Services rules, regulations and policies to the Consultant and to assist in the correction of problem areas identified by the State's monitoring activities

6. LICENSING AND STANDARD COMPLIANCE:
The Consultant agrees to comply in full with all licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance in which the service and/or care is provided for the duration of this agreement. Liability resulting from noncompliance with licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance or through the Consultant's failure to ensure the safety of all individuals served is assumed entirely by the Consultant.

7. ASSURANCE REQUIREMENTS:
The Consultant agrees to abide by all applicable provisions of the following assurances: Lobbying Activity, Debarment and Suspension, Drug-Free Workplace, Executive Order 11246 Equal Employment Opportunity, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Section 504 of the Rehabilitation Act of 1973, Title IX of the Education Amendments of 1972, Drug Abuse Office and Treatment Act of 1972, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Age Discrimination Act of 1975, Americans with Disabilities Act of 1990, Pro-Children Act of 1994, Hatch Act, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Charitable Choice Provisions and Regulations, and American Recovery and Reinvestment Act of 2009 as applicable.

8. RETENTION AND INSPECTION OF RECORDS:
The Consultant agrees to maintain or supervise the maintenance of records necessary for the proper and efficient operation of the program, including records and documents regarding applications, determination of eligibility (when applicable), the provision of services, administrative costs, statistical, fiscal, other records, and information necessary for reporting and accountability required by the State. The Consultant shall retain such records for six years following termination of this agreement. If such records are under pending audit, the Consultant agrees to hold such records for a longer period upon notification from the State. The State, through any authorized representative, will have access to and the right to examine and copy all records, books, papers or documents related to services rendered under this Agreement. State Proprietary Information retained in Consultant's secondary and backup systems will remain fully subject to the obligations of confidentiality stated herein until such information is erased or destroyed in accordance with Consultant's established record retention policies.

All payments to the Consultant by the State are subject to site review and audit as prescribed and carried out by the State. Any over payment of this contract shall be returned to the State within thirty days after written notification to the Consultant.

9. WORK PRODUCT:
The Consultant shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all Services furnished by the Consultant and any subcontractors, if applicable, under this Agreement. It shall be the duty of the Consultant to assure that the services and the system are technically sound and in conformance with all pertinent Federal, State and local statutes, codes, ordinances, resolutions and other regulations. The Consultant shall, without additional compensation, correct or revise any errors or omissions in its work products.

Consultant hereby acknowledges and agrees that all reports, plans, specifications, technical data, drawings, software system programs and documentation, procedures, files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, State Proprietary Information, State Data, End User Data, Personal Health Information, and all information contained therein provided to the State by the Consultant in connection with its performance of service under this Contract shall belong to and is the property of the State and will not be used in any way by the Consultant without the written consent of the State.

Paper, reports, forms software programs, source code(s) and other materials which are a part of the work under this Contract will not be copyrighted without written approval of the State. In the unlikely event that any copyright does not fully belong to the State, the State none the less reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, and otherwise use, and to authorize others to use, any such work for government purposes.

Consultant agrees to return all information received from the State to State's custody upon the end of the term of this contract, unless otherwise agreed in a writing signed by both parties.

10. TERMINATION:
This Agreement may be terminated by the State upon thirty (30) days written notice. This agreement may be terminated by the Vendor for cause with the cause explained by the Vendor in writing and upon one hundred and eighty (180) days written notice. The Vendor is obligated to give the State one hundred and eighty (180) days written notice in the event the Vendor intends not to renew the contract or intends to raise any fees or costs associated with the Vendor's products or services in a subsequent contract unless such fees or costs have previously been negotiated and included in this contract. In the event the Vendor breaches any of the terms or conditions hereof, this Agreement may be terminated by the State at any time with or without notice. Upon notice of termination of a contract or upon reaching the end of the term of this contract unless the contract is renewed, the State of South Dakota requires that State applications that store information to repositories not hosted on the State's infrastructure require the vendor before termination (whether initiated by the State or the Vendor) to extract the State's information such that the State is able to be load the information onto\into repositories listed in the State's Standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's Standard repositories the information (metadata (data structure descriptions) and data) will be extracted into a text file format and returned to the State. Upon the effective date of the termination of the agreement the State of South Dakota again requires that State applications that store information to repositories not hosted on the State's infrastructure require the vendor before termination (whether initiated by the State or the Vendor) to extract the State's information such that the state is able to load the information onto or into repositories listed in the State's Standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's Standard repositories the information (metadata (data structure descriptions) and data) will be extracted into a text file format and returned to the State. If termination for such a default is effected by the State, any payments due to Vendor at the time of termination may be adjusted to cover any additional costs to the State because of Vendor's default. Upon termination the State may take over the work and may award another party an agreement to complete the work under this Agreement. In the event of termination or at the end of the term of this contract unless the contract is renewed, the Vendor shall deliver to the State all reports, plans, specifications, technical data, and all other information completed prior to the date of termination. If after the State terminates for a default by Vendor it is determined that Vendor was not at fault, then the Vendor shall be paid for eligible services rendered and expenses incurred up to the date of termination. The terms of this provision were arrived at after negotiation between the parties. This provision is the joint product or work of the parties, and not a provision written or demanded by any one party to this agreement. The Vendor recognizes and agrees, however, that the State of South Dakota cannot enter into an agreement providing for hosting of any of its data on the Vendor's servers and networks without provisions protecting its ability to access and recover its data in a usable, non-proprietary format in the event of termination of this contract with sufficient time to convert that data and the business functions provided by the Vendor to another system and vendor.

11. FUNDING:
This Contract depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of the law or federal funds reduction, this Contract will be terminated by the State. Termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State.

12. AMENDMENTS:
This Contract may not be assigned without the express prior written consent of the State. This Contract may not be amended except in writing, which writing shall be expressly identified as a part hereof, and be signed by an authorized representative of each of the parties hereto.

13. CONTROLLING LAW:
This Contract shall be governed by and construed in accordance with the laws of the State of South Dakota. Any lawsuit pertaining to or affecting this Agreement shall be venued in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

14. SUPERCESSION:
All other prior discussions, communications and representations concerning the subject matter of this Contract are superseded by the terms of this Contract, and except as specifically provided herein, this Contract constitutes the entire agreement with respect to the subject matter hereof.

15. IT STANDARDS:
Consultant warrants that the software and hardware developed or purchased for the state will be in compliance with the BIT Standards including but not limited to the standards for security, file naming conventions, executable module names, Job Control Language, systems software, and systems software release levels, temporary work areas, executable program size, forms management, network access, tape management, hosting requirements, administrative controls, and job stream procedures prior to the installation and acceptance of the final project. BIT standards can be found at http://bit.sd.gov/standards/.

16. SEVERABILITY:
In the event that any provision of this Contract shall be held unenforceable or invalid by any court of competent jurisdiction, such holding shall not invalidate or renderunenforceable any other provision hereof.

17. NOTICE:
Any notice or other communication required under this Contract shall be in writing and sent to the address set forth above. Notices shall be given by and to the Division being contracted with on behalf of the State, and by the Consultant, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

18. SUBCONTRACTORS:
The Consultant may not use subcontractors to perform the services described herein without express prior written consent form the State. The State reserves the right to reject any person from the contract presenting insufficient skills or inappropriate behavior.

The Consultant will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Contract, any code developed by a subcontractor or agent must be as secure as code developed by the contractor, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Contract. The Consultant will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance. The State, at its option, may require the vetting of any subcontractors. The Consultant is required to assist in this process as needed.

19. HOLD HARMLESS:
The Consultant agrees to hold harmless and indemnify the State of South Dakota, its officers, agents and employees, from and against any and all actions, suits, damages, liability or other proceedings which may arise as the result of performing services hereunder. This section does not require the Consultant to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees.

20. INSURANCE:
Before beginning work under this Contract, Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Contract. The Consultant, at all times during the term of this Contract, shall obtain and maintain in force insurance coverage of the types and with the limits listed below. In the event a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Consultant agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Consultant shall furnish copies of insurance policies if requested by the State.

A. Commercial General Liability Insurance:
Consultant shall maintain occurrence-based commercial general liability insurance or an equivalent form with a limit of not less than $1,000,000 for each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this Contract or be no less than two times the occurrence limit.

B. Business Automobile Liability Insurance:
Consultant shall maintain business automobile liability insurance or an equivalent form with a limit of not less than $500,000 for each accident. Such insurance shall include coverage for owned, hired, and non-owned vehicles.

C. Worker's Compensation Insurance:
Consultant shall procure and maintain Workers' Compensation and employers' liability insurance as required by South Dakota law.

D. Professional Liability Insurance:
Consultant agrees to procure and maintain professional liability insurance with a limit not less than $1,000,000.

(Medical Health Professional shall maintain current general professional liability insurance with a limit of not less than one million dollars for each occurrence and three million dollars in the aggregate. Such insurance shall include South Dakota state employees as additional insureds in the event a claim, lawsuit, or other proceeding is filed against a state employee as a result of the services provided pursuant to this Contract. If insurance provided by Medical Health Professional is provided on a claim made basis, then Medical Health Professional shall provide "tail" coverage for a period of five years after the termination of coverage.)

21. CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:
Consultant certifies, by signing this agreement, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by the federal government or any state or local government department or agency. Consultant further agrees that it will immediately notify the State if during the term of this Contract either its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

22. CONFLICT OF INTEREST:
Consultant agrees to establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal organizational conflict of interest, or personal gain.

23. REPORTING PROVISION:
Consultant agrees to report to the State any event encountered in the course of performance of this Contract which results in injury to any person or property, or which may otherwise subject Consultant, or the State of South Dakota or it officers, agents or employees to liability. Consultant shall report any such event to the State immediately upon discovery.
Consultant's obligation under this section shall only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. Consultant's obligation to report shall not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section shall not excuse or satisfy any obligation of Consultant to report any event to law enforcement or other entities under the requirements of any applicable law.

24. CONFIDENTIALITY OF INFORMATION:
For the purpose of the sub-paragraph, "State Proprietary Information" shall include all information disclosed to the Consultant by the State. Consultant acknowledges that it shall have a duty to not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. Consultant shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this contract; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this contract; (iii) make State Proprietary Information available to any of its employees, officers, agents or consultants except those who have agreed to obligations of confidentiality at least as strict as those set out in this contract and who have a need to know such information. Consultant is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. Consultant shall protect confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. State Proprietary Information shall not include information that (i) was in the public domain at the time it was disclosed to Consultant; (ii) was known to Consultant without restriction at the time of disclosure from the State; (iii) that is disclosed with the prior written approval of State's officers or employees having authority to disclose such information; (iv) was independently developed by Consultant without the benefit or influence of the State's information; (v) becomes known to Consultant without restriction from a source not connected to the State of South Dakota. State's Proprietary Information shall include names, social security numbers, employer numbers, addresses and all other data about applicants, employers or other clients to whom the State provides services of any kind. Consultant understands that this information is confidential and protected under applicable State law at SDCL 1-27-1.5, modified by SDCL 1-27-1.6, SDCL 28-1-29, SDCL 28-1-32, and SDCL 28-1-68 as applicable federal regulation and agrees to immediately notify the State if the information is disclosure, either intentionally or inadvertently. The parties mutually agree that neither of them shall disclose the contents of the contract except as required by applicable law or as necessary to carry out the terms of the contract or to enforce that party's rights under this contract. Consultant acknowledges that the State and its agencies are public entities and thus are bound by South Dakota open meetings and open records laws. It is therefore not a breach of this contract for the State to take any action that the State reasonably believes is necessary to comply with the South Dakota open records or open meetings laws. If work assignments performed in the course of this Agreement require additional security requirements or clearance, the Consultant will be required to undergo investigation.

25. HANDLING OF DATA BREACHES:
Immediately upon becoming aware of a data compromise or of circumstances that could have resulted in unauthorized access to, disclosure of, alternation of, or use of State data, Vendor will notify the State, fully investigate the incident, and cooperate fully with the State's investigation of, analysis of, and response to the incident. The vendor will use a forensics company that is acceptable to the State, preserve all evidence including but not limited to communications, documents, and logs and the State will have the authority to set the scope of the investigation. In addition, the Vendor shall inform the State of the actions it is taking or will take to reduce the risk of further loss to the State.

Except as otherwise required by law, Vendor shall provide notice of the incident to the State only. The State shall then give notice to the person or entity whose data may have been involved, to regulatory agencies, and to other entities. This procedure is adopted for the purpose of promoting clarity of reporting and avoiding confusion and double reporting.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to the State under law or equity, the Vendor will reimburse the State in full for all costs incurred by the State in investigation and remediation of such Data Compromise, including but not limited to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract. The Vendor shall also reimburse the State in full for all costs the State incurs in its offering of 1 year credit monitoring to each person whose data were compromised. The Vendor shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Data Compromise.

26. CHANGE MANAGEMENT PROCESS:
From time to time it may be necessary or desirable for either the State or the Contractor to propose changes in the Services provided. Such changes shall be effective only if they are in writing and contain the dated signatures of authorized representatives of both parties. Unless otherwise indicated, a change or amendment shall be effective on the date it is signed by both parties. Automatic upgrades to any software used by the Contractor to provide any services that simply improve the speed, efficiency, reliability, or availability of existing services and do not alter or add functionality, are not considered "changes to the Services" and such upgrades will be implemented by the Contractor on a schedule no less favorable than that provided by the Contractor to any other customer receiving comparable levels of services.

27. CURING OF BREACH OF AGREEMENT:
In the event of a breach of these representations and warranties, Consultant shall immediately, after telephonic notice from the State, begin work on curing such breaches. If such problem remains unresolved after three days, at State's discretion, Consultant will send, at Consultant's sole expense, at least one qualified and knowledgeable representative to the State's site where the system is located. This representative will continue to address and work to remedy the deficiency, failure, malfunction, defect, or problem at the site. The rights and remedies provided in this paragraph are in addition to any other rights or remedies provided in this Agreement or by law.

28. RESELLING SOFTWARE:
The Vendor is acting as reseller for (Company name here) of their product (Product name here). As such the Vendor has attached to this agreement as exhibit ____ all the licensing requirements of (Company name here) including any End User License Agreements that apply to (Product name here). The state will not be bound by any End User License Agreements that are not incorporated into this contract. This includes those agreements that require as part of the install or use of a product a 'click agree to continue' or similar type of process. In such cases, the state acknowledging or agreeing to terms not included in writing in this agreement shall reflect only a step required in the install or use process for the product and shall create no further obligation for the state beyond what is included in this agreement. The Vendor will provide the needed planning and installation documents for the state to follow in implementing and managing the product and certifies that for (Product name here) all the licensing requirements of (Company name here) being purchased through this agreement will be met if the state adheres to the planning documents provided. This certification will be performed before (Product name here)'s installation and reviewed in a technical walk-through before Vendor is paid for the acquisition of (Product name here) and its installation. In case of conflict this clause to take precedence over any other agreement.

If (company name here) makes any changes in the licensing requirements for (Product name here) the reseller must notify the State in writing of these changes at least (6) six-months in advance of the renewal or of the normal termination of this agreement, whichever occurs first. If the licensing changes are made within the (6) six-month period then the State must be notified in writing of these changes immediately. For these changes to be in affect the changes must be added to the renewal contract as signed by the State. Any contract terms that are referenced in the contract but not included in writing as part of the renewal contract signed by the State are null and void

29. BROWSER:

The system, site, and/or application must be compatible with the State's current browser standard which can be found at, http://bit.sd.gov/standards/. PHP or Adobe ColdFusion will not be used in the system, site, and/or application.

30. INSTALLATION AND OPERATION OF THE PRODUCT:
The State will install and operate the Vendor's product on the State's computing infrastructure. The State's installation process and operation of the product will follow current State standards. Those standards can be found at http://bit.sd.gov/standards/. It is the Vendor's responsibility to review these standards and alert the state if the costs enumerated in the contract will change based on state standards. The state will not be responsible for added licensing or processing costs if the Vendor determines at a later date that by following the standards in effect at the time of installation the state is or would be obligated to pay fines; additional rates; fees; license costs or charges of any type; additional charges of any type or character for Vendor's or a third party's intellectual property; or added support costs.

31. SECURITY:
The Vendor shall take all actions necessary to protect state information from exploits, inappropriate alterations, access or release, and malicious actor attacks.
By signing this contract, the Vendor warrants that:

A. All known security issues are resolved.

B. Assistance will be provided to the State of South Dakota by the Vendor in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. This investigation can include security scans made at the State's discretion. Failure by the Vendor to remedy any security issues discovered can be considered a breach of this contract by the State.

The state applies security patches and security updates as needed to maintain compliance with industry best practices as well as state and federal audit requirements. Vendors who do business with the state must also keep up with industry security practices and requirements. Vendors must include costs and time needs in their proposals and project plans to assure they can keep up with all security needs throughout the life-cycle of a project. The state will work in good faith with vendors to help them understand and support state security requirements during all phases of a project's life-cycle but will not assume the costs to mitigate applications or processes that fail to meet then-current security requirements.

At the state's discretion, security scanning will be performed and or security settings put in place or altered during the software development phase and during pre-production review for new or updated code. These scans and tests, initially applied to development and test environments, can be time consuming and should be allowed for in project planning documents and schedules. Products not meeting the State's security and performance requirements will not be allowed into production and will be barred from User Acceptance Testing (UAT) until all issues are addressed to the state's satisfaction. The discovery of security issues during UAT are automatically grounds for non-acceptance of a product even if a product meets all other acceptance criteria. Any security issues discovered during UAT that require product changes will not be considered a project change chargeable to the state. The state urges the use of industry scanning/testing tools and secure development methods be employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the software entity producing or delivering an application to the state. Unless expressly indicated in writing, the state assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing.

Consistent with the provisions of this Contract, the Vendor, subcontractor and or agent throughout shall use the highest applicable industry standards for sound secure software development practices to resolve critical security issues as quickly as possible. These standards include but are not limited to the South Dakota Application Security Vulnerabilities document which can be found at http://cybersecurity.sd.gov/docs/development/DevelopmentSecurityItems.pdf. Items listed under Section A of the South Dakota Security Vulnerabilities document may not be present. Continued compliance of these standards is required as the standards will change over time. The "highest applicable industry standards" shall also be defined as the degree of care, skill, efficiency, and diligence that a prudent person possessing technical expertise in the subject area and acting in a like capacity would exercise in similar circumstances.

At the State's discretion the State will discuss the security controls used by the State with the Vendor upon the Vendor signing a non-disclosure agreement.

32. MALICIOUS CODE:
The Vendor covenants that:

A. The Licensed Software does not contain any code that does not support a software requirement.

B. Will not insert into the Licensed Software or any media on which the Licensed Software is delivered any virus, rogue program, time bomb, worm, Trojan Horse, back doors, Easter eggs or other malicious or intentionally destructive code.

C. Will use commercially reasonable efforts consistent with industry standards to scan for and remove any Malicious Code from the Licensed Software before installation. In the event any Malicious Code is discovered in the Licensed Software as delivered by the Vendor to the State under this contract, the Vendor shall provide the State at no charge with a clean copy of the applicable Licensed Software that does not contain such Malicious Code or otherwise correct the affected portion of the services provided to the State under this contract. The remedies in this paragraph are in addition to such other and additional remedies as the State may have at law equity or otherwise.

D. Will resolve all known security issues.

33. DENIAL OF ACCESS OR REMOVAL OF AN APPLICATION FROM PRODUCTION
During the life of this contract the application can be denied access to or removed from the production system at BIT's discretion. The reasons for the denial of access or removal of the application from the production system can include, but are not limited to, security, functionality, unsupported third party technologies, or excessive resource consumption. At the discretion of the State contractual payments may be suspended while the application is denied access to or removed from the production system if the problem is caused by the Vendor's actions or inactions. Access to the production system and any updates to the production system will be made only with BIT's prior approval. It is expected that any fixes will be tested on the test system provided by the Vendor as stated in the RFP and not on the production system. It is expected that the Vendor shall provide BIT with proof of the fix proposed before BIT provides access to the production system. The certification by BIT of the fix on the test system does not guarantee the Vendor access to the production system. BIT shall sign a non-disclosure agreement with the Vendor if revealing its fix will put the Vendor's intellectual property at risk. If the Vendor is unable to produce the project deliverables due to the Vendor actions or inactions within thirty (30) days of the application's denial of access or removal from the production system and the Vendor does not employ the change management process to alter the project schedule or deliverables within the same thirty (30) days then at the State's discretion the contract may be terminated and Vendor is required to refund to the State all contractual payments made to that point

34. MOVEMENT OF PRODUCT:
The State operates a virtualized computing environment and retains the right to use industry standard hypervisor high availability, fail-over, and disaster recovery systems to move instances of the product(s) between the install sites defined with the Vendor provided resource and usage restrictions as outlined elsewhere in The Agreement are maintained. This movement of product can be done by the State without any additional fees or charges by the Vendor. As part of normal operations the State may also install the product on different computers or servers if the product is also removed from the previous computer or server provided resource and usage restrictions as outlined elsewhere in The Agreement are maintained. This movement of product can be done by the State without any additional fees or charges by the Vendor.

35. USE OF PRODUCT ON VIRTUALIZED INFRASTRUCTURE AND CHANGES TO THAT INFRASTRUCTURE:

The State operates a virtualized computing environment and uses software-based management and resource capping to fulfill licensing obligations and retains the right to use and upgrade as deemed appropriate its hypervisor and operating system technology and related hardware to execute the product without additional license fees or other charges provided the state assures the guest operating system(s) running within that hypervisor environment continue to present computing resources to the licensed product that conform with the terms of the license agreement. The computing resource allocations within the state's hypervisor software-based management controls for the guest operating system(s) executing the product shall be the only consideration in licensing compliance related to computing resource capacity.

36. LOAD BALANCING

The State routinely load balances applications that run on the State's computing environment across multiple servers. The Vendor's product must be able to be load balanced across multiple servers. Any changes or modifications required to allow the Vendor's product to be load balanced so that it can operate on the State's computing environment will be at the Vendor's expense.

37. SOFTWARE FUNCTIONALITY AND REPLACEMENT

The software licensed by the Vendor to the State provides the functionality as outlined in Section 3, Scope of Work, in the Request for Proposal, as incorporated herein.

The Vendor agrees that:

A. If in the opinion of the State the Vendor reduces or replaces the functionality contained in the licensed product, and provides this functionality as a separate or renamed product, then the State shall be entitled to license such software product at no additional license or maintenance fee;

B. If in the opinion of the State the Vendor releases an option, future product, purchasable product or other release that has substantially the same functionality as the software product licensed to the State, and it ceases to provide maintenance for the older software product, and then the State shall have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the vendor discontinues the licensed product and recommends movement to a new product as a replacement option regardless of any additional functionality the replacement product may have over the licensed product.

38. BACKUP COPIES:

The State may make and keep backup copies of the licensed product without additional cost or obligation on the condition that:

1) The State keeps possession of the backup copies;
2) The backup copies are only used as bona fide backups.

39. USE OF ABSTRACTION TECHNOLOGIES:

The Vendor's application must use appropriate abstraction technologies, such as relative pathing. By way of example, hardcoded server names and hardcoded IP addresses are not permitted.

Use of hard-coded resources may result in a failure to pass pre-production testing or may cause the application to fail or be shut down at any time without warning. In all such cases, correcting the hardcoding violations shall be the responsibility of the Vendor and will not be a project change chargeable to the State.

40. LICENSE GRANT AND SCOPE OF USE:

A. The Vendor grants to the State a worldwide, nonexclusive license to use the software and associated documentation, plus any additional software which shall be added by mutual agreement of the parties during the term of this contract.
B. The license usage model is based on ______________________.
C. The license grant shall be extended to any contractors, subcontractors, outsourcing vendors, consultants and others who have a need to use the software for the benefit of the State.

D. There shall be no limit on the number of machines, number of locations, or size of processors on which he State can operate the software.

E. There shall be no limit on the operating systems upon which the software may be used on.

F. The State has the right to use industry standard hypervisor high availability, fail-over, and disaster recovery systems to move instances of the software between installation sites.

41. LICENSE AGREEMENTS:

Vendor warrants that it has provided to the State and incorporated into this agreement all license agreements, end user agreements, and terms of use regarding its software or any software incorporated into its software before execution of this Agreement. The parties agree that neither the State nor its end users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. This paragraph shall control and supersede the language of any such agreements to the contrary.

42. SOFTWARE AUDIT:

Not more than once per year, Vendor may ask State to deliver to Vendor periodic usage reports generated from specific products (when available) or written reports, whether generated manually or electronically, specifying State's use of Vendor's software product. If after reviewing the usage reports, Vendor believes that State is not in compliance with the terms of this Agreement, Vendor may, upon thirty (30) days' prior written notice, request an audit of State's use of the software product.

A. In its request for the audit, but in no event less than thirty (30) days prior to the date for the audit, Vendor must deliver to State documentation that outlines the following:

a. Vendor's proposed process to determine usage

b. Anticipated timeline

c. Any work, reports or documentation which Vendor expects State to provide

d. Any software, code or scripts which Vendor expects State to install, run or access State systems, all of which will be subject to the State's prior approval which approval may be conditioned on any or all of the following:

i. Compliance with the State's data privacy and security protocols:

ii. Compliance with the State's data privacy and security protocols;

iii. Utilization in a test environment without damage or threat to the State system;

iv. Vendor's agreement to indemnify, defend and hold harmless State from any damages caused by such software, code or scripts, including, but not limited to, consequential damages such as loss or impaired use of the State system.

e. The method used to match software usage against software entitlements

f. What constitutes proof of ownership of software entitlements

g. Vendor's records on software entitlements currently held by State

B. State reserves the right to determine when and how samples will be used in the audit, instead of complete inspection. State must agree in advance to the methods which will be used to interpolate results from samples

C. If necessary, Vendor may, at its sole cost, and subject to the availability and workload of State personnel and Vendor's compliance with State's access and security policies and procedures, access State's facilities during normal business hours to perform the audit.

D. Vendor shall deliver a copy of the audit report to State, and will, at the State's request, mask any sensitive information included in the report. Vendor shall include the number of entitlements which can be used for any future audits in the audit report.

E. State shall have thirty (30) days from receipt of the audit report from Vendor to review the audit and challenge the findings in writing. If State challenges any or all of the findings, the parties shall meet and work in good faith to resolve the issues. If the parties are unable to resolve the issues either party may pursue its rights at law and in equity.

F. State has thirty (30) days from the date of the final audit report to correct any perceived problems where the software was not or is not actually being used without paying any additional license fees or penalty under the software license agreement. For example, State may correct the problem by: removing the software from unused servers, removing software that had been downloaded in error, removing software that had been downloaded or installed but never used.

G. Vendor shall continue to provide technical maintenance and support during the entire audit process through resolution of all usage issues so long as State is enrolled in Vendor Support. Vendor shall not in any way disrupt any other technical maintenance or support in any way related to the product.

H. If Vendor's final audit report reveals that State has exceeded the licensed capacity of a product, State shall pay the applicable license and support fees for the excess licenses that are not subject to removal under F) above, at the previously contracted price without any penalty. Such payment will be made within a reasonable time, which must be calculated to allow the State to seek appropriate funding .

I. Vendor may, with prior written approval of State, in its sole discretion, have a third party, chosen by mutual agreement with State (other than Business Software Alliance, FAST, or the Software and Information Industry Association), conduct the audit under an appropriate confidentiality agreement. In order to protect the integrity of the audit, Vendor must agree to compensate the third party on a basis other than penalties assessed or recovered or a percentage of the penalties assessed or recovered. Vendor must compensate the third party at a rate that does not change based on the outcome of the audit.

All information or findings from the audit are highly confidential to the State and subject to the confidentiality provisions of this Agreement. This clause supersedes any and all other agreements the Vendor may have with the State concerning Vendor software audits.

43. DISCLOSURE OF OPEN SOURCE, CUSTOM BUILT AND PROPRIETARY TECHNOLOGIES:
Technology vendors must grant the State the right to perform scanning and audits on their processes, tools and systems. These scans and audits may be software-based and/or involve interviews, remote access sessions, on-site tours, reviews of key contracts, self-attestation processes, as well as other reasonable means of gathering and validating information. The State will make reasonable efforts to ensure that these audits and scans minimize the impact on the Vendor's business operations.

Refusal to comply with this request may be grounds to exclude a vendor from consideration as a technology provider for the State's confidential, sensitive, or private data or systems. Falsifying or withholding information requested by the State may, at the State's sole discretion, be deemed a breach of contract by the Vendor and/or an automatic exclusion from consideration or selection in an RFP process. Regardless, the Vendor remains solely responsible for any penalties, fines or legal actions that may result from the falsification or withholding of information.

The Vendor must disclose to the State using Exhibit ____all tools, systems, third-party products, and services used in the development, support, maintenance, hosting, accessing, authenticating, encrypting, storing, retrieving, backing up, recovering, sharing, and accessing of any and all data, systems, workflows, and any other technologies used by the Vendor at or on any site, location, or system that supports or is co-located with systems or data belonging to or in use by the State. This includes technologies that are open source, custom built, and proprietary.

The State will, at the Vendor's written request, sign a non-disclosure statement provided that the request is deemed to comply with the following South Dakota open records laws and exceptions:
http://legis.sd.gov/Statutes/Codified_Laws/DisplayStatute.aspx?Type=Statute&Statute=1-27-1.1
http://legis.sd.gov/Statutes/Codified_Laws/DisplayStatute.aspx?Type=Statute&Statute=1-27-1.3.
http://legis.sd.gov/Statutes/Codified_Laws/DisplayStatute.aspx?Type=Statute&Statute=1-27-30

44. MOBILE APPLICATIONS:
The Vendor's application is required to; (i) only reuse code within the boundaries and guidelines of State Standards; (ii) encrypt data in transport and at rest using a mutually agreed upon encryption format; (iii) close all connections and close at the end of processing; (iv) have no code not required for the functioning of

application; (v) have no “Back Doors” or other entries into the application other than those that have the prior approval of the State; (vi) have no tracking of device owner’s activities without a clear notice given to the device owner and requiring the device owner’s active approval before the application does any tracking; (vii) not have connections to any service not required by the functional requirements of the application or defined in the project requirements documentation; (viii) fully disclose in the “About” information the connections made, permission(s) required and the purpose of those connections and permission(s); (ix) only ask for those permissions and access rights on the owner’s device that are required for the defined requirements of the Vendor’s application and (x) have no access to data outside of what is defined in the About information for the Vendor’s application.

45. PERFORMANCE OF ADDITIONAL WORK:
The Vendor will perform additional work on their application at the hourly rate of ______. This work can be authorized by any of the State signatories to this contract. This additional work will not be considered a project change chargeable to the State if it is for reasons of correcting security deficiencies, meeting the functional requirements established for the application, unsupported third party technologies or excessive resource consumption. Completion of this additional work can be a requirement for an application to go into or stay in production.

46. APPLICATION OF CONTRACT TERMS:
All of the following terms and provisions are applicable to each and every entity that hosts State data. If Vendor subcontracts any hosting of State data to another entity, the relationship between Vendor and any such subcontracting entity must be that of Principal and Agent. No such Agent may act as an independent contractor for Vendor. Vendor must include in its contract with any such Agent explicit terms providing for this Principal and Agent relationship, and Vendor must further supervise such Agent so as to insure that such Agent complies with all of the following terms.

47. THIRD PARTY HOSTING:
If (Vendor name here) has the State’s or end user’s data hosted by another party (Vendor name here) must provide the State the name of this party and the terms of service, agreement or contract (Vendor name here) has with this other party. It is permissible for (Vendor name here) to redact any pricing or cost information from these documents. (Vendor name here) must provide the State with contact information for this third party and the location of their data center(s). (Vendor name here) must receive from the third party written assurances that the state and or end user data will reside in the United States at all times and provide these written assurances to the State. If the terms of service, agreement or contract as well as the location of the data center(s) and the written assurance that the data will reside in the United States is not acceptable to the State the State may terminate this contract and seek another service provider without penalty. Failure to abide by any of these terms will be considered a breach of this contract by (Vendor name here).

48. DISASTER RECOVERY:
The Contractor will maintain a disaster recovery plan (the “Disaster Recovery Plan”) with respect to the services provided to the State. For purposes of this Agreement, a “Disaster” shall mean any unplanned interruption of the operation of or inaccessibility to the Contractor’s service in which the State, using reasonable judgment, requires relocation of processing to a recovery location. The State shall notify the Contractor as soon as possible after the State deems a service outage to be a Disaster. The Contractor shall move the processing of the State’s services to a recovery location as expeditiously as possible and shall coordinate the cut-over.

49. AUDIT:
The Contractor agrees to one of the following:

A. Allow State, at Vendor’s expense, twice annually, a security audit and vulnerability assessment to provide third party verification of Vendor’s IT security safeguards for the system and its data and/or that of the company and its policies and procedures. At its request, the state may review any and all independent audit reports that document the system’s and company’s policies and/or procedure’s security posture. This security audit and vulnerability assessment must come from a third party source agreed to in advance by the state; or

B. Allow the state at the state's expense to perform up to two security audit and vulnerability assessments per year to provide verification of Vendor's IT security safeguards for the system and its data. The state will work with the Vendor to arrange the audit at a time least likely to create work load issues for the Vendor and will accept scanning a test or UAT environment on which the code and systems are a mirror image of the production environment.

The Vendor agrees to work with the state to rectify any serious security issues revealed by the security audit and vulnerability assessments. This includes additional security audits and vulnerability assessments that shall be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. It is required that any security audits must meet the requirements of the Payment Card Industry Data Security Standard (PCI DSS) irrespective of there being any PCI DSS data involved.

50. RIGHTS AND LICENSE IN AND TO STATE AND END USER DATA:
The parties agree that between them, all rights including all intellectual property rights in and to State and End User data shall remain the exclusive property of the State, and that the Contractor has a limited, nonexclusive license to use these data as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

51. MIGRATION CAPABILITY:
Upon termination or expiration of this Agreement, the Contractor will ensure that all State and End User Data is transferred to the State or a third party designated by the State securely, within a reasonable period of time, and without significant interruption in service, specified in the Request for Proposal. The Contractor will ensure that such migration uses facilities and methods that are compatible with the relevant systems of the transferee, and to the extent technologically feasible, that the State will have reasonable access to State and End User Data during the transition.

The Contractor will notify the State of impending cessation of its business or that of a tiered provider and any contingency plans in the event of notice of such an event. This includes immediate transfer of any previously escrowed assets and data and State access to the Contractor's facilities to remove or destroy any State-owned assets and data. The Contractor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Contractor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Contractor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State. The Contractor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the State, all such work to be coordinated and performed in advance of the formal, final transition date.

52. SUSPENSION OF SERVICES:
The State may suspend, or terminate, or direct the Contractor to suspend or terminate, an End User's access to services in accordance with the State's policies. The State will assume sole responsibility for any claims made by End Users regarding the State's suspension/termination or directive to suspend/terminate such service. The Contractor may suspend access to services to an End User(s) immediately in response to an act or omission that reasonably appears to jeopardize the security or integrity of the Contractor's services or the network(s) or facilities used to provide the services. Suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. The suspension will be lifted immediately when the breach is cured. The Contractor may suspend access to services by an End User in response to a material breach by End User of any terms of use he or she has agreed to in connection with receiving the services. The Contractor will notify the State of any suspension of End User access to services before suspension.

53. HOST NETWORK SECURITY:
The Contractor will use industry standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement as indicated in the Information Technology User Security Guide.

The Contractor will, at its expense, either conduct or have conducted at least on an annual basis and provide to the state upon its request:

A. A vulnerability scan, performed by a scanner approved by the State, of the Contractor's systems and facilities that are used in any way to deliver services under this Agreement; and
B. Formal penetration test, performed by a process and qualified personnel approved by the State, of the Contractor's systems and facilities that are used in any way to deliver services under this Agreement.

54. LEGAL REQUESTS FOR DATA:
Except as otherwise expressly prohibited by law, the Contractor will:

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Contractor seeking State and/or End User Data maintained by the Contractor;
B. Consult with the State regarding its response;
C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request; and
D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

55. EDISCOVERY:
The Contractor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Contractor shall not respond to service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

56. DATA PRIVACY:
The Contractor agrees to the following:

A. The Contractor will use State Data and End User Data only for the purpose of fulfilling its duties under this Agreement and for the State's and its End User's sole benefit, and will not share such data with, or disclose it to, any third party, without the prior written consent of the State or as otherwise required by law. By way of illustration and not of limitation, the Contractor will not use such data for the Contractor's own benefit and, in particular, will not engage in "data mining" of State or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State data.
B. All State and End User Data will be stored on servers located solely within the continental United States.
C. The Contractor will provide access to State and End User Data only to those Contractor employees and subcontractors who need to access the data to fulfill the Contractor's obligations under this Agreement.

57. DATA EXCHANGE AND ENCRYPTED DATA STORAGE:
All facilities used to store and process State and End User data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the

Contractor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Contractor warrants that all State and End User Data will be encrypted in transmission (including via web interface) and storage at no less than 128-bit level encryption,

58. DATA RETENTION AND DISPOSAL:
The Contractor agrees to the following:

A. The Contractor will use commercially reasonable efforts to retain data in an End User's account until the End User deletes them, or for an alternate time period mutually agreed by the parties.
B. Using appropriate and reliable storage media, the Contractor will regularly back up State and End User Data and retain such backup copies for a minimum of thirty-six months. At the end of that time period and at the State's election, the Contractor will either securely destroy or transmit to the State repository the backup copies. Upon the State's request, the Contractor will supply the State with a certificate indicating the nature of the storage media destroyed, the date destroyed, and the method of destruction used.
C. The Contractor will retain logs associated with End User activity for a minimum of seven years, unless the parties mutually agree to a different period.
D. The Contractor will immediately place a "hold" on the destruction under its usual storage media retention policies of storage media that include State and End User Data, in response to an oral or written request from authorized State personnel indicating that those records may be relevant to litigation that the State reasonably anticipates. Oral requests by the State for a hold on storage media destruction will be reproduced in writing and supplied to the Contractor for its records as soon as reasonably practicable under the circumstances. The State will promptly coordinate with the Contractor regarding the preservation and disposition of storage media. The Contractor shall continue to preserve the storage media until further notice by the State. The Contractor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the methods of disposal of storage media, are appropriate to and fulfill all of the State's needs. By way of example but not of limitation, all hard drives and tapes used to store State data must, upon destruction be properly disposed of.

59. SYSTEM UPGRADES:
Advance notice of ___ (to be negotiated) shall be given to the State of any major upgrades or system changes that the Contractor will be implementing. A major upgrade is a replacement of hardware, software or firmware with a newer or better version, in order to bring the system up to date or to improve its characteristics. The State reserves the right to postpone these changes.

60. SEPARATION OF JOB DUTIES:
The Contractor shall require commercially reasonable non-disclosure agreements, and limit staff access to State data to that which is required to perform job duties.

61. PROVISION OF SERVICES:
The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided.

62. IDENTIFICATION OF BUSINESS PARTNERS:
The Contractor shall identify all of its business partners and subcontractors related to services provided. under this contract, who will be involved in any application development and/or operations.

63. REMOVAL OF CONTRACTOR REPRESENTATIVE:
The State shall have the right at any time to require that the Contractor remove from the project any staff or subcontractor who the State believes is detrimental to the project. The State will provide the Contractor with notice of its determination, and the reasons it requests the removal. If the State signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual.

64. LOCATION OF STATE AND END USER DATA:

All State data hosted by the contractor will be stored in facilities located in the United States of America. At no time is it acceptable for any State data to be stored in facilities outside the United States of America. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the United States of America.

65. AUTHORIZED SIGNATURES**:**
In witness hereto, the parties signify their agreement by affixing their signatures hereto.

____ ______________
Consultant Signature Date

____ ______________
State – DSS Deputy Secretary Brenda Tidball-Zeltinger Date

State Agency Coding:

CFDA # ____________ ____________ ____________ ____________
Company ____________ ____________ ____________ ____________
Account ____________ ____________ ____________ ____________
Center Req ____________ ____________ ____________ ____________
Center User ____________ ____________ ____________ ____________
Dollar Total ____________ ____________ ____________ ____________
____________ ____________ ____________ ____________

DSS Program Contact Person ______________________________
Phone ____________

DSS Fiscal Contact Person Patty Hanson
Phone 605 773-3586

Consultant Program Contact Person ______________________________
Phone ____________

Consultant Fiscal Contact Person ______________________________
Phone ______________________________
Consultant Email Address ______________________________

SDCL 1-24A-1 states that a copy of all consulting contracts shall be filed by the State agency with the State Auditor within five days after such contract is entered into and finally approved by the contracting parties. For further information about consulting contracts, see the State Auditor's policy handbook.

Tools and Infrastructure Worksheet

Contractor/Vendor Name: ___________________________ Date: _______

Product Name: ___________________________

Name of person filling out this form: ___________________________

Title of person filling out this form: ___________________________

Phone Number: ___-___-____ Email address: ___________________________

Instructions:
Provide the information below for all tools, systems, third-party products, and services used in the development, support, maintenance, hosting, accessing, authenticating, encrypting, storing, retrieving, back up, recovery, sharing, and accessing of state data, systems, workflows, and any other data related technologies used by the Vendor supporting services offered to the State. This includes technologies that are open source, custom built, and proprietary
A separate form must be filled out for each product or service(s) the State will be licensing. Services/products provided by third parties must be included. If you have any questions please contact your BIT point of contact.

Name of the process or software	Source of process or software	URL of webpage for the source of the process or software (If available and applicable)	Purpose or function of the process or software

Attachment B

Vendor Questions

Add text detail as required

1	**Typically the State of South Dakota prefers to host all systems. In the event that the State decides that it would be preferable for the vendor to host the system, is this an option?**	**Yes☐ No☐ NA** ☐
2	Is there a workstation install requirement?	Yes☐ No☐ NA ☐
3	Is this a browser based User Interface?	Yes☐ No☐ NA ☐
4	What is the development technologies used for this system? ASP Version: ______ NET Version: ______ Java/JSP Version: ______ Other? Describe: ________________________ Version: ________________________	
5	Will the system support authentication?	Yes☐ No☐ NA ☐
6	Will the system infrastructure require an email interface?	Yes☐ No☐ NA ☐
7	Will the system require a database?	Yes☐ No☐ NA ☐
8	Will the system infrastructure require database replication?	Yes☐ No☐ NA ☐
9	Will the system require transaction logging for database recovery?	Yes☐ No☐ NA ☐
10	Will the system infrastructure have a special backup requirement?	Yes☐ No☐ NA ☐
11	Will the system provide an archival solution? If not is the State expected to develop a customized archival solution?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐
12	Will the system infrastructure have any processes that require scheduling?	Yes☐ No☐ NA ☐
13	Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?	Yes☐ No☐ NA ☐
14	Will the system infrastructure require a Business Intelligence solution?	Yes☐ No☐ NA ☐
15	Will the system have any workflow requirements?	Yes☐ No☐ NA ☐

16	Explain the software licensing model.	
17	Is there a documented disaster recovery plan?	Yes□ No□ NA □
18	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?	Yes□ No□ NA □
19	Can the system be implemented via Citrix?	Yes□ No□ NA □
20	Will the system implement its own level of security?	Yes□ No□ NA □
21	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?	Yes□ No□ NA □
22	Will the system print to a Citrix compatible networked printer?	Yes□ No□ NA □
23	Will the network communications meet IEEE standard TCP/IP and use either standard ports or State defined ports as the State determines?	Yes□ No□ NA □
24	Will the system provide Internet security functionality on Public portals including encrypted network/secure socket layer. (TLS 1.0/SSL 3.0)?	Yes□ No□ NA □
25	Will the system provide Internet security functionality on a public portal to include firewalls?	Yes□ No□ NA □
26	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies, would this affect the implementation of the system?	Yes□ No□ NA □
27	If your application uses Java is it locked into a certain version or will it use the latest version if so what is your process for updating the application?	Yes□ No□ NA □
28	If your application does not run under the latest Microsoft operating system what is your process for updating the application?	
29	Will the server based software support: a. Windows server 2008R2 or higher b. IIS7.0 or higher c. MS SQL Server 2008R2 or higher d. Exchange 2010 or higher e. Citrix presentation server 4.5 or higher f. VMWare ESX 4.1 or higher g. MS Windows Updates h. Symantec End Point Protection	Yes□ No□ NA □ Yes□ No□ NA □ Yes□ No□ NA □ Yes□ No□ NA □ Yes□ No□ NA □ Yes□ No□ NA □ Yes□ No□ NA □ Yes□ No□ NA □
30	Identify each of the Data, Business and Presentation layer technologies your product would use and provide a roadmap outlining how your release and or update roadmap aligns with the release and or update roadmap for this technology.	
31	All network systems must operate within the current configurations of the State of South Dakota's firewalls, switches, firewalls, IDS/IPS and desktop security infrastructure. Would this affect the implementation of the system?	Yes□ No□ NA □

32	It is State policy that all systems must be compatible with BITs dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?	Yes☐ No☐ NA ☐
33	It is State policy that all systems that require an email interface must leverage existing SMTP processes currently managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐
34	It is State policy that all Vendor/Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Secure Gateway. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐
35	It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐
36	It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. If need is determined by the State, would this affect the implementation of the system?	Yes☐ No☐ NA ☐
37	The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐
38	It is State policy that all access from outside of the State of South Dakota's private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐
39	It is State policy that systems must support NAT and PAT running inside the State Network. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐
40	It is State policy that systems must not use dynamic TCP or UDP ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would this affect the implementation of the system?	Yes☐ No☐ NA ☐
41	Will your system use Adobe Air, Adobe Flash, Apache Flex, JavaFX , Microsoft Silverlight? If yes what are your plans for moving off them?	Yes☐ No☐ NA ☐
42	Does your web application use PHP or Adobe ColdFusion?	Yes☐ No☐ NA ☐
43	Does your system require 3rd party add-ons, plug-ins, or special requirements to do calculations and or data processing on the workstation?	Yes☐ No☐ NA ☐
44	How does data enter the system (transactional or batch or both)?	
45	Is the system data exportable by the user for use in tools like Excel or Access?	Yes☐ No☐ NA ☐

46	Will user customizable data elements be exportable also?	Yes☐ No☐ NA ☐
47	Will the system distinguish between local versus global administrators where local administrators have rights to user management only for the program area that they are associated with and global administrators have rights for the entire system?	Yes☐ No☐ NA ☐
48	Will this system provide the capability to track data entry/access by the person, date and time?	Yes☐ No☐ NA ☐
49	Will the system provide data encryption for sensitive information both in storage and transmission?	Yes☐ No☐ NA ☐
50	It is State policy that systems at the discretion of the State may have a Security Audit performed on it by BIT or a 3rd Party for security vulnerabilities. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐
51	The Vendors/Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the state's discretion a vendor's answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the vendor selection criteria. Is this acceptable?	Yes☐ No☐ NA ☐
52	The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?	Yes☐ No☐ NA ☐
53	Will the vendor provide assistance with installation?	Yes☐ No☐ NA ☐
54	Is there an installation guide available and will you provide a copy to the State?	Yes☐ No☐ NA ☐
55	Is telephone assistance available for both installation and use?	Yes☐ No☐ NA ☐
56	Is on-site assistance available? If so, is there a charge?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐
57	Will the implementation plan include user acceptance testing?	Yes☐ No☐ NA ☐
58	Will technical documentation for application maintenance purposes be provided to the State?	Yes☐ No☐ NA ☐
59	Will the State be given test cases for regression testing of custom developed software	Yes☐ No☐ NA ☐
60	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?	Yes☐ No☐ NA ☐
61	List and describe all training modules you have to offer and the intended audience for each training module.	
62	Can the user manual be printed?	Yes☐ No☐ NA ☐
63	Is the user manual electronically available?	Yes☐ No☐ NA ☐

64	Is there on-line help assistance available?	Yes☐ No☐ NA ☐
65	Describe your Support options.	
66	Is there a method established to communicate availability of system updates?	Yes☐ No☐ NA ☐
67	Is there an established method to acquire system updates?	Yes☐ No☐ NA ☐
68	The State implements enterprise wide anti-virus solutions on all servers and workstations as well as controls the roll-outs of any and all Microsoft patches based on level of criticality. Do you have any concerns in regards to this process?	Yes☐ No☐ NA ☐
69	Will you provide customization of the system if required by the State of South Dakota?	Yes☐ No☐ NA ☐
70	Will the state be required to develop customized interfaces to other applications?	Yes☐ No☐ NA ☐
71	Will the State be required to develop reports or data extractions from the database?	Yes☐ No☐ NA ☐
72	Do you have a formal change management process?	Yes☐ No☐ NA ☐
73	Will the State of South Dakota have access to the underlying data and data model for ad hoc reporting purposes?	Yes☐ No☐ NA ☐
74	Will the source code for the system be put in escrow for the State of South Dakota?	Yes☐ No☐ NA ☐
75	If the source code is placed in escrow, will the vendor pay the associated escrow fees?	Yes☐ No☐ NA ☐
76	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?	Yes☐ No☐ NA ☐
77	Explain the basis on which pricing could change for the state based on your licensing model.	
78	Contractually, how many years price lock are you offering the state as part of your response? Also as part of your response, how many additional years are you offering to limit price increases and by what percent?	
79	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?	Yes☐ No☐ NA ☐
80	Has your company ever conducted a project where you were tasked with performing load testing?	Yes☐ No☐ NA ☐
81	Has your company ever developed a system that ran on Citrix Metaframe?	Yes☐ No☐ NA ☐
82	Have you ever created a User Acceptance Test plan and test cases?	Yes☐ No☐ NA ☐

83	It is State policy that all Vendor/Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Secure Gateway. Would this affect the implementation of the system? If the policy above is not acceptable, will your proposed VPN Connections meet the following requirements: o Pre-Shared Key o AES (256bits or Higher) o SHA1 o No PFS or Aggressive Modes allowed.	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐
84	Are there expected periods of time where the application will be unavailable for use?	Yes☐ No☐ NA ☐
85	Is there a strategy for mitigating unplanned disruptions?	Yes☐ No☐ NA ☐
86	Will the State of South Dakota own the data created in your hosting environment?	Yes☐ No☐ NA ☐
87	Will the State acquire the data at contract conclusion?	Yes☐ No☐ NA ☐
88	Will organizations other than the State of South Dakota have access to our data?	Yes☐ No☐ NA ☐
89	Will the State's data be used for any other purposes other than South Dakota's usage?	Yes☐ No☐ NA ☐
90	Will the State's data be protected?	Yes☐ No☐ NA ☐
91	Is your software consistent with State standards?	Yes☐ No☐ NA ☐
92	List any third-party software or any hardware required to run your proposed solution	

Appendix C

Security Vendor Questions

Security Vendor Questions - COTS Software Set

Commercial-off-the-shelf (COTS) software is a term for software products that are ready-made and are readily available for purchase in the commercial market. The table below lists questions to consider asking during a COTS software evaluation.

Anything “Not Applicable” should be marked “NA”.

#	Question	Comments
Software History and Licensing		
1	Can the pedigree of the software be established? Briefly explain what is known of the people and processes that created the software.	
2	Explain the change management procedure that identifies the type and extent of changes conducted on the software throughout its lifecycle.	
3	Is there a clear chain of licensing from original author to latest modifier. Describe the chain of licensing.	
4	What assurances are provided that the licensed software does not infringe upon any copyright or patent? Explain	
5	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Provide a brief explanation. Will the supplier indemnify the Acquirer from these issues in the license agreement? Provide a brief explanation.	
Development Process Management		

#	Question	Comments
6	What are the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers) techniques, etc. used to produce and transform the software (brief summary response)?	
7	What security measurement practices and data does your company use to assist product planning?	
8	Is software assurance considered in all phases of development? Explain	
Software Security Training and Awareness		
9	Describe the training your company offers related to defining security requirements, secure architecture and design, secure coding practices, and security testing.	
10	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?	
11	Describe the company's policy and process for professional certifications and ensuring certifications are valid and up-to date.	
Concept and Planning		
12	Are there some requirements for security that are "structured" as part of general releasability of a product and others that are "as needed" or "custom" for a particular release?	
13	What process is utilized by your company to prioritize security related enhancement requests?	
Architecture and Design		
14	What threat assumptions were made, if any, when designing protections for the software and information assets processed?	
15	What security design and security architecture documents are prepared as part of the SDLC process?	
16	How are design documents for completed software applications archived?	
Software Development		

#	Question	Comments
17	What are/were the languages and non-developmental components used to produce the software (brief summary response)?	
18	What secure development standards and/or guidelines are provided to developers?	
19	Are tools provided to help developers verify that the software they have produced software that is minimized of weaknesses that could lead to exploitable vulnerabilities? What is the breadth of common software weaknesses covered (e.g., specific CWEs)?	
20	In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?	
Built-in Software Defenses		
21	Does the software validate (e.g., filter with white listing) inputs from untrusted sources before being used?	
22	Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user) and is it designed to isolate and minimize the extent of damage possible by a successful attack?	
23	Does the documentation explain how to install, configure, and/or use it securely? Does it identify options that should not normally be used because they create security weaknesses?	
24	Where applicable, does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?	
25	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used? Are legal agreements in place to protect against potential liabilities of nonsecure software?	
Component Assembly		

#	Question	Comments
26	What security criteria, if any, are considered when selecting third-party suppliers?	
27	Is the software required to conform to coding or API standards in any way? Explain.	
Testing		
28	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing, integrated testing)?	
29	Who and when are security tests performed on the product? Are tests performed by an internal test team, by an independent third party, or by both?	
30	What degree of code coverage does your testing provide?	
31	Are misuse test cases included to exercise potential abuse scenarios of the software?	
32	Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?	
33	What release criteria does your company have for its products with regard to security?	
Software Manufacture and Packaging		
34	What security measures are in place for the software packaging facility?	
35	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?	
36	How is the software packaged (e.g. Zipped , Linux RPM etc) and distributed?	
37	How is the integrity of downloaded software (if an option) protected?	
38	For the released software "object", how many "files" does it consist of? How are they related?	
Installation		
39	Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration following installation? If so, how is it obtained?	

#	Question	Comments
40	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?	
Assurance Claims and Evidence		
41	How has the software been measured/assessed for its resistance to identified, relevant attack patterns? Are Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs) used? How have the findings been mitigated?	
42	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If the CC, what evaluation assurance level (EAL) was achieved? If the product claims conformance to a protection profile, which one(s)? Are the security target and evaluation report available?	
43	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?	
44	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?	
45	Has the product undergone any penetration testing? When? By whom? Are the test reports available under a nondisclosure agreement? How have the findings been mitigated?	
46	Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)?	
Support		

#	Question	Comments
47	Is there a Support Lifecycle Policy within the organization for the software in question? Does it outline and establish a consistent and predictable support timeline?	
48	How will patches and/or Service Packs be distributed to the Acquirer?	
49	What services does the help desk, support center, or (if applicable) online support system offer?	
Software Change Management		
50	How extensively are patches and Service Packs tested before they are released?	
51	Can patches and Service Packs be uninstalled? Are the procedures for uninstalling a patch or Service Pack automated or manual?	
52	Will configuration changes (if needed for the installation to be completed) be reset to what was there before the patch was applied in cases where the change was not made explicitly to close a vulnerability?	
53	How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?	
54	Do you determine relative severity of defects and does that drive other things like how fast you fix issues?	
55	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches?	
56	Are your version control and configuration management policies and procedures the same throughout your entire organization and for all your products? How are they enforced? Are third-party developers contractually required to follow these policies and procedures?	
57	What policies and processes does your company use to verify that software components do not contain unintended, “dead,” or malicious code? What tools are used?	

#	Question	Comments
58	How is the software provenance verified (e.g. any checksums or signatures)?	
Timeliness of Vulnerability Mitigation		
59	Does your company have a vulnerability management and reporting policy? Is it available for review?	
60	Does your company publish a security section on its Web site? If so, do security researchers have the ability to report security issues?	
Security "Track Record"		
61	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?	
Financial History and Status		
62	Has your company ever filed for Recompany under U.S. Code Chapter 11? If so, please provide dates for each incident and describe the outcome.	
63	Does your company have policies and procedures for periodically reviewing the financial health of the third-party entities with which it contracts for software development, maintenance, or support services?	
64	Does your company have established policies and procedures for dealing with the contractual obligations of third-party developers that go out of business?	

Security Vendor Questions- Custom Application Set

Custom software is software developed either for a specific organization or function that differs from other already available software. It is generally not targeted to the mass market but rather is usually created for specific Agencies or Business Areas.

Anything “Not Applicable” should be marked “NA”.

#	Questions	Comments
Software History and Licensing		
1	Can the software pedigree be established? What is known of the people and processes that created the software (brief summary response)?	
2	Is there a change management procedure or document that will identify the type and extent of changes conducted on the software throughout its lifecycle?	
3	What assurances are provided that the software does not infringe upon any copyright or patent?	
4	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Will the supplier indemnify the Acquirer from these issues in the license agreement?	
Development Process Management		
5	What are the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers) techniques, etc. used to produce and transform the software (brief summary response)?	
6	What security measurement practices and data does your company use to assist project planning?	
7	Is software assurance considered in all phases of development?	
8	How is software risk managed? Are anticipated threats identified, assessed, and prioritized?	
Software Security training and Awareness		

#	Questions	Comments
9	What training does your company offer related to defining security requirements, secure architecture and design, secure coding practices, and security testing?	
10	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?	
11	Describe the company's policy and process for professional certifications and for ensuring certifications are valid and up-to date.	
Concept and Planning		
12	Are there some requirements for security that are "structured" as part of general releasability of an application and others that are "as needed" or "custom" for a particular release?	
13	Are there some requirements for quality that are "structured" as part of general releasability of an application and others that are "as needed" or "custom" for a particular release?	
14	What review processes are implemented to ensure that nonfunctional requirements are unambiguous, traceable and testable throughout the entire SDLC?	
15	Are security requirements developed independently of the rest of the requirements engineering activities, or are they integrated into the mainstream requirements activities?	
16	Are misuse/abuse cases derived from the application requirements? Are relevant attack patterns used to identify and document potential threats?	
17	What tool(s) does your company use for requirements management?	
18	If an agile development method is used, how formally are requirements documented?	
Architecture and Design		
19	What threat modeling process, if any, is used when designing the software protections?	
20	What analysis, design, and construction tools are used by your software design teams?	
21	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to\\for review?	
Software Development		

#	Questions	Comments
22	What languages and non-developmental components are used to produce the software (brief summary response)?	
23	Does your company have formal coding standards for each language in use? If yes, how are they enforced? How often are these standards and practices reviewed and revised?	
24	Does the software development plan include security peer reviews?	
25	Are tools provided to help developers verify that the software they have produced software that is minimized of weaknesses that could lead to exploitable vulnerabilities? What is the breadth of common software weaknesses covered (e.g., specific CWEs)?	
26	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of the documentation of this methodology or provide information on how to obtain it from a publicly accessible source.	
27	Does your organization establish contractually binding agreements with their own developers and/or with their third-party developers regarding the ownership and/or licensing of intellectual property?	
28	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?	
29	Are there contractual recourses that the organization can take if a third-party developer delivers software that contains malicious code?	
30	Does the organization ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of "trigger" events.	

#	Questions	Comments
31	In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?	
Built-in Software Defenses		
32	Does the software validate (e.g., filter with white listing) inputs from untrusted sources before being used?	
33	Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user) and is it designed to isolate and minimize the extent of damage possible by a successful attack?	
34	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?	
35	Does the exception-handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?	
36	Does the documentation explain how to install, configure, and/or use it securely? Does it identify options that should not normally be used because they create security weaknesses?	
37	Where applicable, does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?	
38	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used? Are legal agreements in place to protect against?	
Component Assembly		
39	Does the software have any security critical dependencies or need additional controls from other software (e.g., operating system, directory service, applications), firmware, or hardware? If yes, please describe.	

#	Questions	Comments
40	Is the software regularized to conform to coding or API standards in any way?	
41	Is delivery of demonstrably secure software a contractual requirement for third-party developed software? If yes, what criteria are used to operationally define "secure software"?	
42	Are additional risk management measures in place in the software's design to mitigate risks posed by use of third-party components?	
Testing		
43	What types of functional tests are performed on the software during its development (e.g., spot checking, component-level testing, security testing, integrated testing)?	
44	Does your company's defect classification schemes include security categories? During testing what proportion of identified defects relate to security?	
45	What degree of code coverage does your testing provide?	
46	Are misuse test cases included to exercise potential abuse scenarios of the software?	
47	Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?	
48	When does security testing occur during the SDLC (e.g., unit level, subsystem, system, certification and accreditation)?	
Installation		
49	If you are responsible for installing the software, is this done by your organization or through third-party consultants?	
50	Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration following installation?	
51	What training/documentation is available for software installation and maintenance?	
Assurance Claims and Evidence		

#	Questions	Comments
52	Does your company develop security measurement objectives for phases of the SDLC? Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?	
53	Has the software been measured/assessed for its resistance to identified relevant attack patterns? Are Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumeration (CWEs) used? How have the findings been mitigated?	
54	Are static or dynamic software security analysis tools used to identify the weaknesses that can lead to exploitable vulnerabilities in the software? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?	
55	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?	
56	Has the software undergone any penetration testing? When? By whom? Are the test reports available under a nondisclosure agreement? How have the findings been mitigated?	
57	Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)?	
58	How is the assurance of software produced by third-party developers assessed?	
Support		
59	Are multiple tiers of support contracts available? If yes, please describe the support plans available.	
60	Is there a Support Lifecycle Policy for the software in question? Does it outline and establish a consistent and predictable support timeline?	
61	How will patches and/or Service Packs be distributed to the Acquirer?	

#	Questions	Comments
62	How are trouble tickets submitted? How are support issues, specifically those that security related, escalated?	
63	Are help desk or support center personnel internal company resources or are these services outsourced to third parties?	
64	If help desk or support center services are outsourced to third parties, are they located in foreign countries?	
Software Change management		
65	What are your policies and procedures for maintaining development documents, including requirements, design and architecture documents, source code, binaries, and user documentation?	
66	Are your version control and configuration management policies and procedures the same throughout your entire organization? How are they enforced? Are third-party developers contractually required to follow these policies and procedures?	
67	Are configuration/change controls in place to prevent unauthorized modifications or additions to source code and related documentation? Do these controls detect and report unexpected modifications/additions to source code? Do they aid in rolling back an affected artifact to a pre-modified version?	
68	Are there any undocumented features present not intended for use by end users, but available for use by the supplier for technical support and development?	
69	How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?	
70	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches?	

#	Questions	Comments
71	Does your organization have policies and procedures in place to monitor and audit the transmission of its technology-related intellectual property to third parties, and to prevent unauthorized transmission of that intellectual property?	
72	What policies and processes does your organization use to verify that software components do not contain unintended, "dead," or malicious code? What tools are used?	
73	Is a process utilized by your company that can be used for documenting and analyzing the security aspects of fielded systems and for steering future improvements and modifications to those systems?	
Timeliness of Vulnerability Mitigation		
74	Does your company have a vulnerability management and reporting policy? Is it available for review?	
Individual Malicious Behavior		
75	Does your company perform background checks on members of the software development team? If so, are there any additional "vetting" checks done on people who work on critical application components, such as security? Explain.	
76	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle, along with management oversight and enforcement? Explain.	
77	What training is available to your development staff to help them identify malicious behavior? Are there formal policies for reporting malicious behavior?	
78	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.	
Organizational History		

#	Questions	Comments
79	Please summarize your company's history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).	
80	Please provide a list of the names and dates of service of the following executive officers: • Chairman of the Board (COB) • Chief Executive Officer (CEO) • President (if different from CEO) • Vice President(s) • Chief Financial Officer (CFO)	
81	How many employees does your company have: • In the U.S.? • Worldwide?	
Foreign Interests and Influences		
82	Is the controlling share (51+%) of your company owned by a non-U.S. entity? If so, please complete Standard Form 328, Certificate Pertaining to Foreign Interests.	
83	Is your company an entity of a larger "parent" company? If yes" does that "parent" company include any subsidiaries or other sub-entities that are 51+% foreign owned? If so, please identify those subsidiaries/sub-entities.	
84	Please provide company names of all third-party entities with whom your firm contracts software development, maintenance, or support services related to this procurement.	
Financial History and Status		
85	Has your company ever filed for Recompany under U.S. Code Chapter 11? If so, please provide dates for each incident and describe the outcome.	
86	What are your company's policies and procedures for periodically reviewing the financial health of the third-party entities with which it contracts for software development, maintenance, or support services?	
87	What are your company's policies and procedures for dealing with the contractual obligations of third party developers that go out of business?	

Security Vendor Questions - Hosted Application Set

Increasingly, software is executed and maintained by someone other than the acquirer and provided as a service to them. Application service providers host the servers that support the applications in a data center and provide different levels of service, including security-related services. Users remotely access the software. Suppliers should also ask software development questions for the appropriate software type to augment the questions below.

Anything "Not Applicable" should be marked "NA".

#	Questions	Comments
Service Confidentiality Policies		
1	What are your customer confidentiality policies? How are they enforced?	
2	What are your customer privacy policies? How are they enforced?	
3	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?	
4	What are the set of controls to ensure separation of data and security information between different customers that are physically located in the same data center? On the same host server?	
Operating Environment for Services		
5	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?	
6	What are your policies and procedures for hardening servers?	
7	What are your data backup policies and procedures? How frequently are your backup procedures verified?	
8	What are the procedures for evaluating any vendor security alerts and installing patches and Service Packs?	
9	How are vendor patches and Services Packs applied?	

10	Is testing done after changes are made to servers? What are your rollback procedures in the event of problems resulting from installing a patch or Service Pack?	
11	What are the agents or scripts executing on servers of hosted applications? Are there procedures for reviewing the security of these scripts or agents?	
12	What are the procedures and policies used to approve, grant, monitor and revoke access to the servers? Are audit logs maintained?	
13	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?	
14	Do you have a formal disaster recovery plan? What actions will be taken to recover from a disaster? Are warm or hot backups available?	
15	What are the procedures used to approve, grant, monitor, and revoke file permissions for production data and executable code?	
16	Is two-factor authentication used for administrative control of all security devices and critical information systems?	
Security Service Available		
17	What are the types of information security services you provide?	
18	How are virus prevention, detection, correction, and updates handled for the products?	
19	What type of firewalls (or application gateways) do you use? How are they monitored/managed?	
20	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?	
21	Is your system and network architecture based on a high availability design that includes redundant firewalls, routers, switches and IDS, and load balanced or clustered servers?	
Security Monitoring		

22 Do you perform regular reviews of system and network logs for security issues?

23 Do you have an automated security event management system?

24 What are your procedures for intrusion detection, incident response, and incident investigation/escalation?

25 Will you provide on-site support 24x7 to resolve security incidents?

26 Do you provide write-once technology for storing audit trails and security logs?

27 How do you control physical and electronic access to the log files? Are log files consolidated to single servers?

28 Do you provide security performance measures to the customer at regular intervals?

Assurance Claims and Evidence

29 Has functional security testing been performed on the services?

30 Do you perform penetration testing of the service? If yes, how frequently are penetration tests performed? Are the tests performed by internal resources or by a third party?

31 Do you provide automated vulnerability testing of the service? If yes, how frequently are the tests performed? Are the tests performed by internal resources or by a third party?